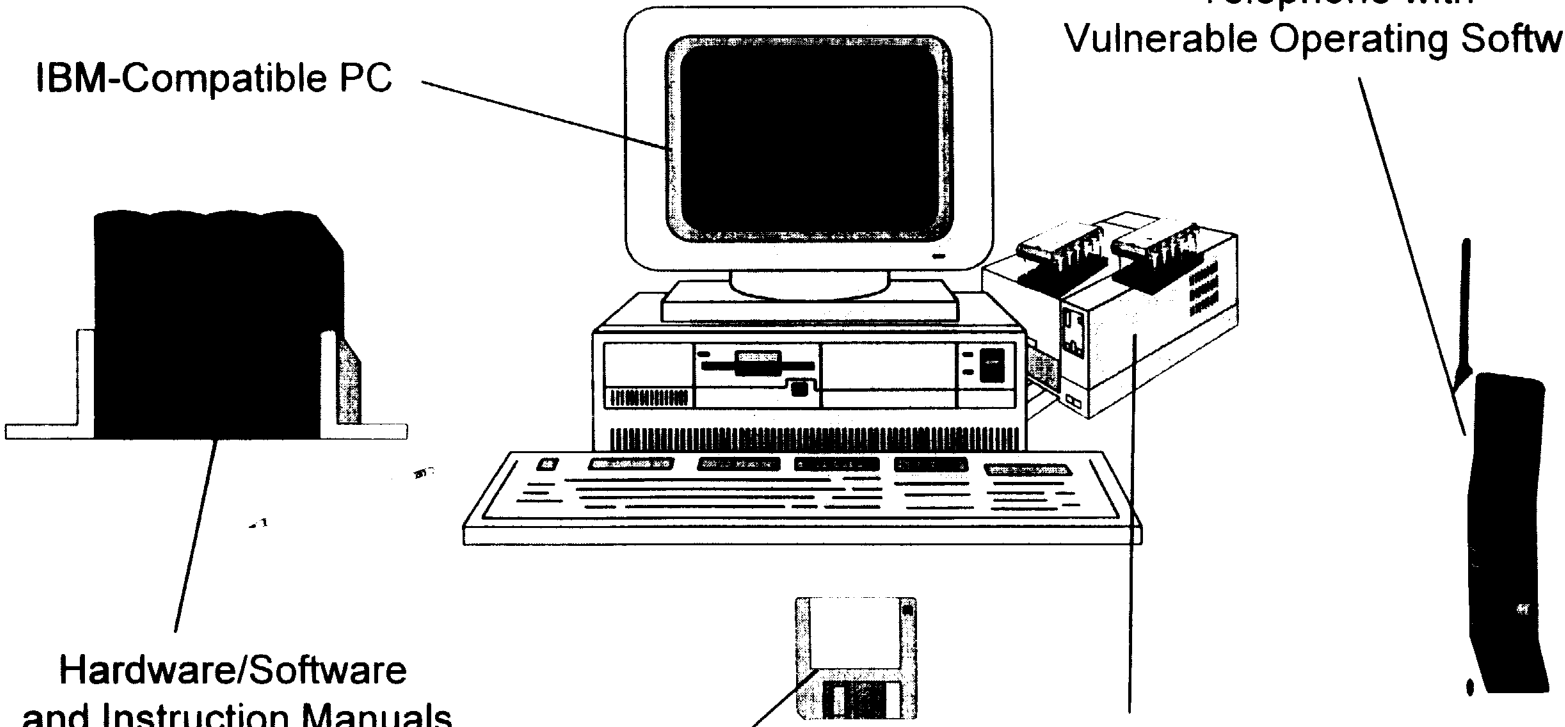
Typical Class C Counterfeiting



Telephone with Vulnerable Operating Software

IBM-Compatible PC

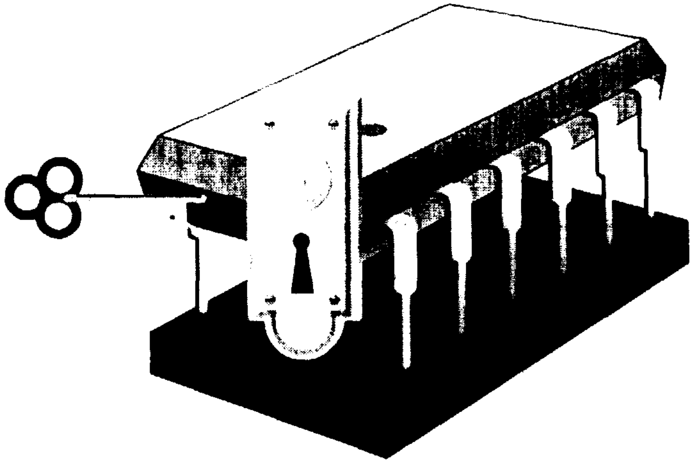
Hardware/Software and Instruction Manuals

Disassembly and EPROM Programming Software

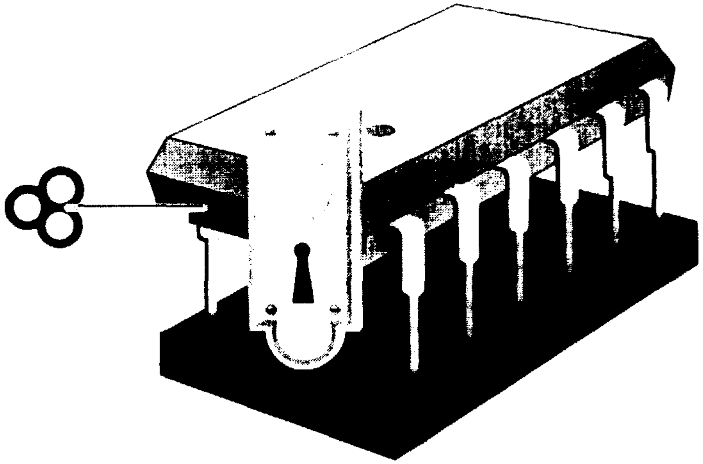
EPROM Programmer and Chips

Technical Efforts to Enhance Telephone Security

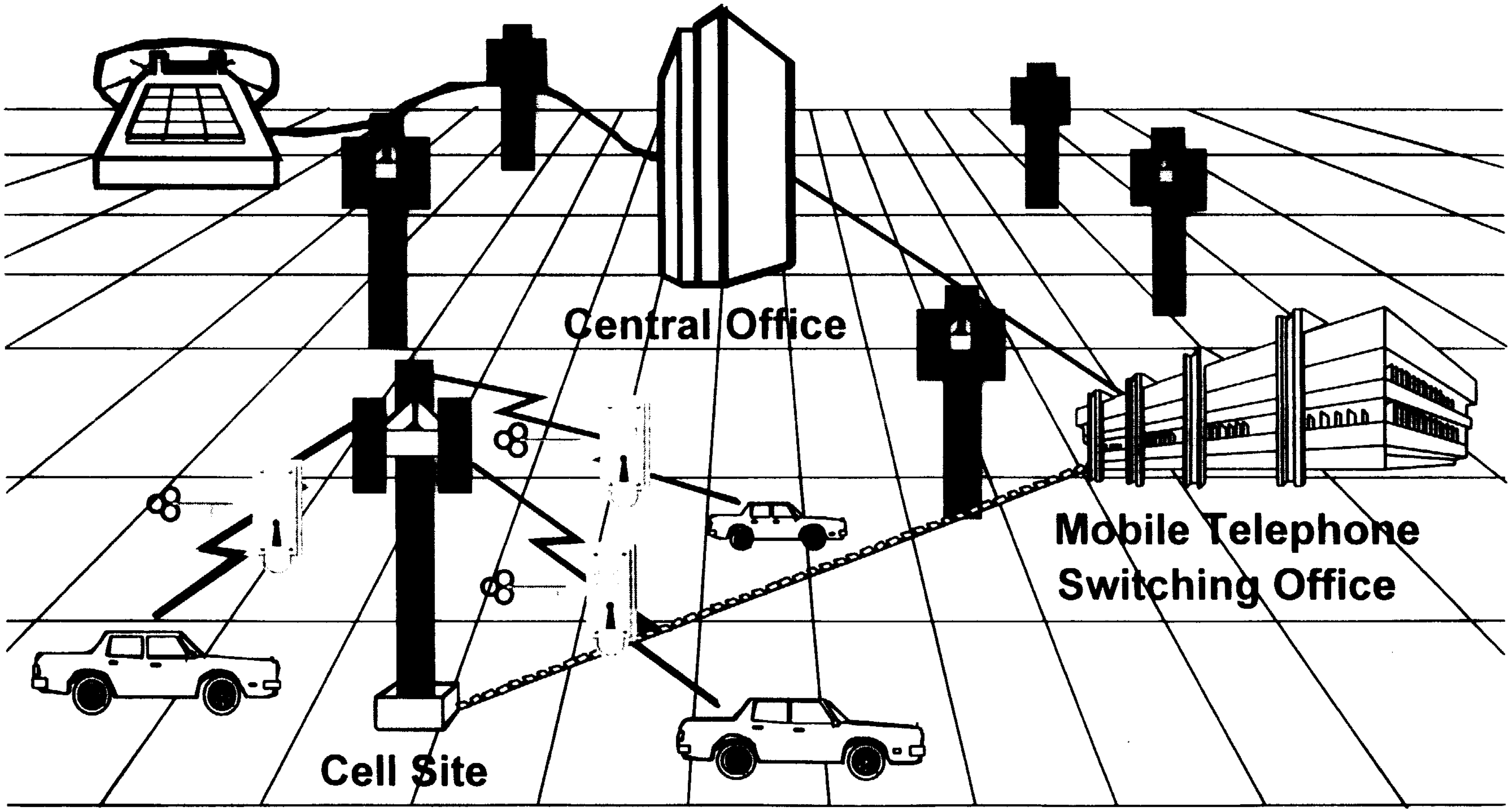
ESN Storage



Firmware Storage

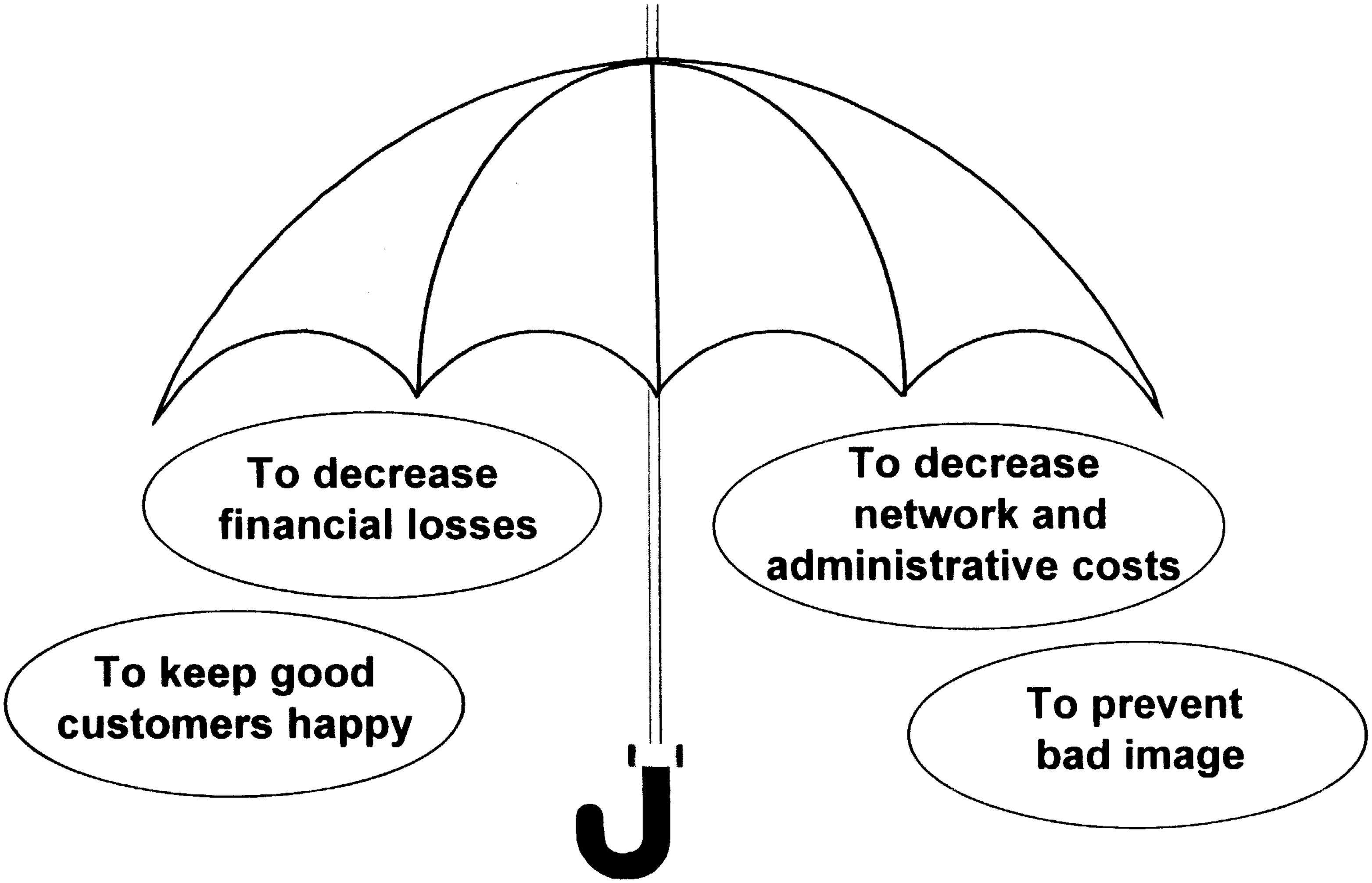


Cellular Fraud Control – Locking the Radio Path



700–3

Why Reduce and Manage Fraud?



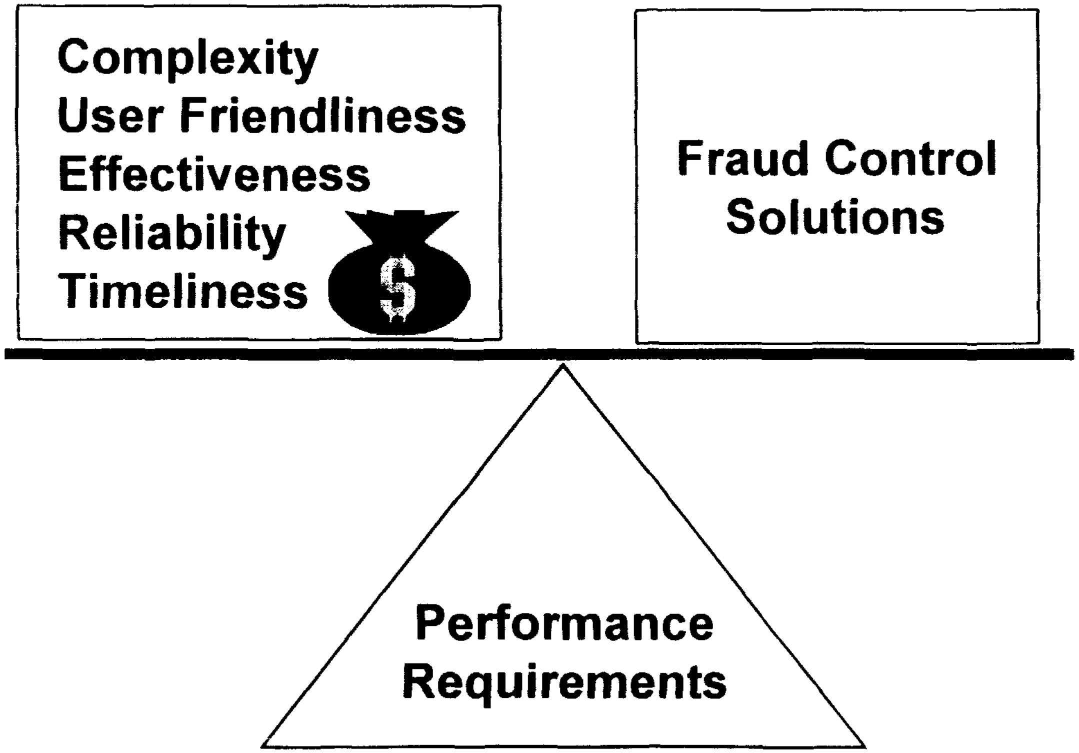
To decrease financial losses

To decrease network and administrative costs

To keep good customers happy

To prevent bad image

Balancing Fraud and Business Operations



Complexity
User Friendliness
Effectiveness
Reliability
Timeliness

Fraud Control Solutions

Performance Requirements

Existing Technologies for Fraud Management

- Pre-call validation of every call
- Post-call validation of every call
- Expert system-based call detail analysis systems (CloneDetector)
- Personal Identification Number (PIN) identification techniques – "Fraud Prevention Features"

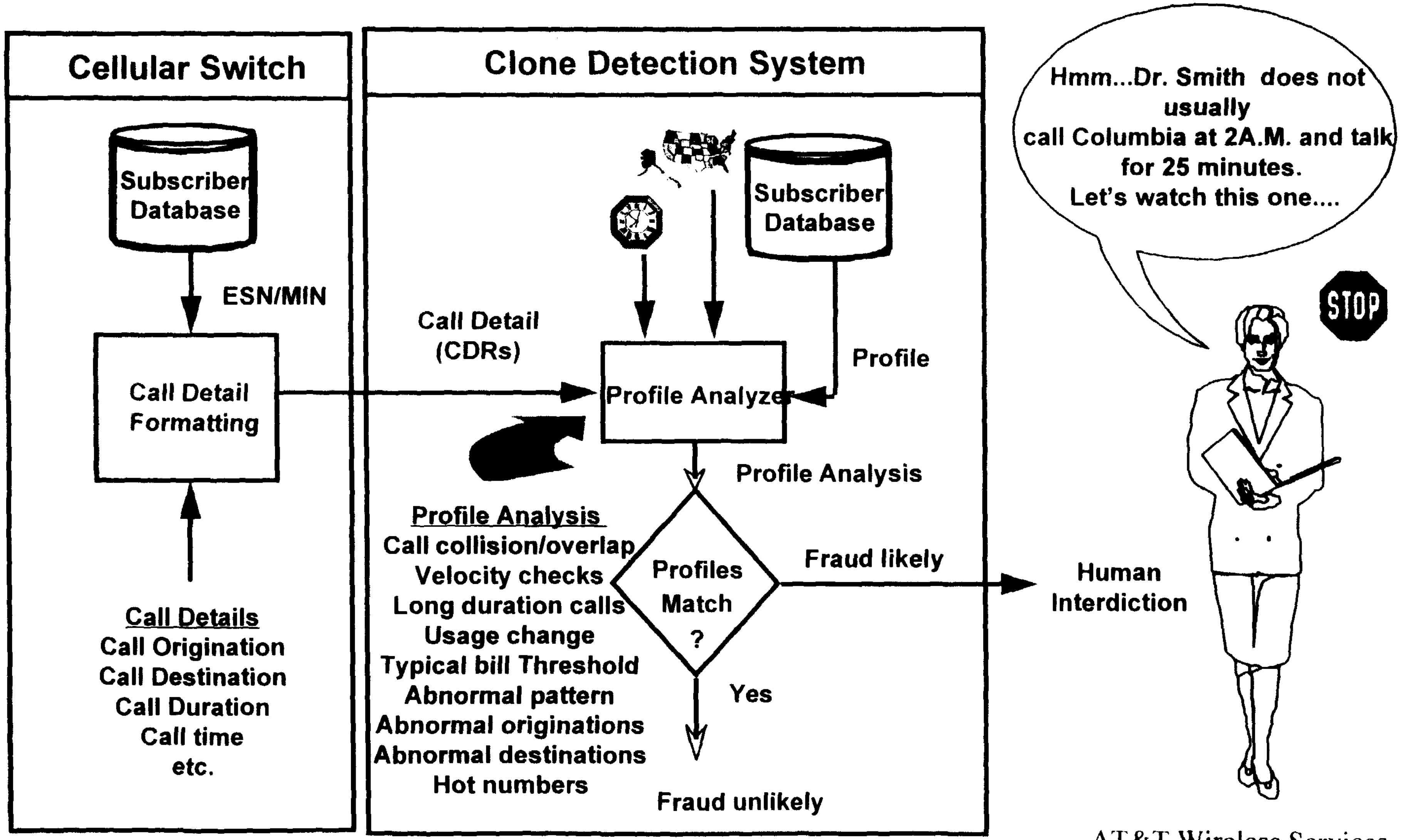
Fraud Products and Services

- Profiling “CloneDetector” System
- FraudManager Service
- HLR Visibility
- Stolen Phone StatCheck Service
- Customer Positive File Service
- Positive Validation Service (PVS)

Emerging Technologies for Fraud Management

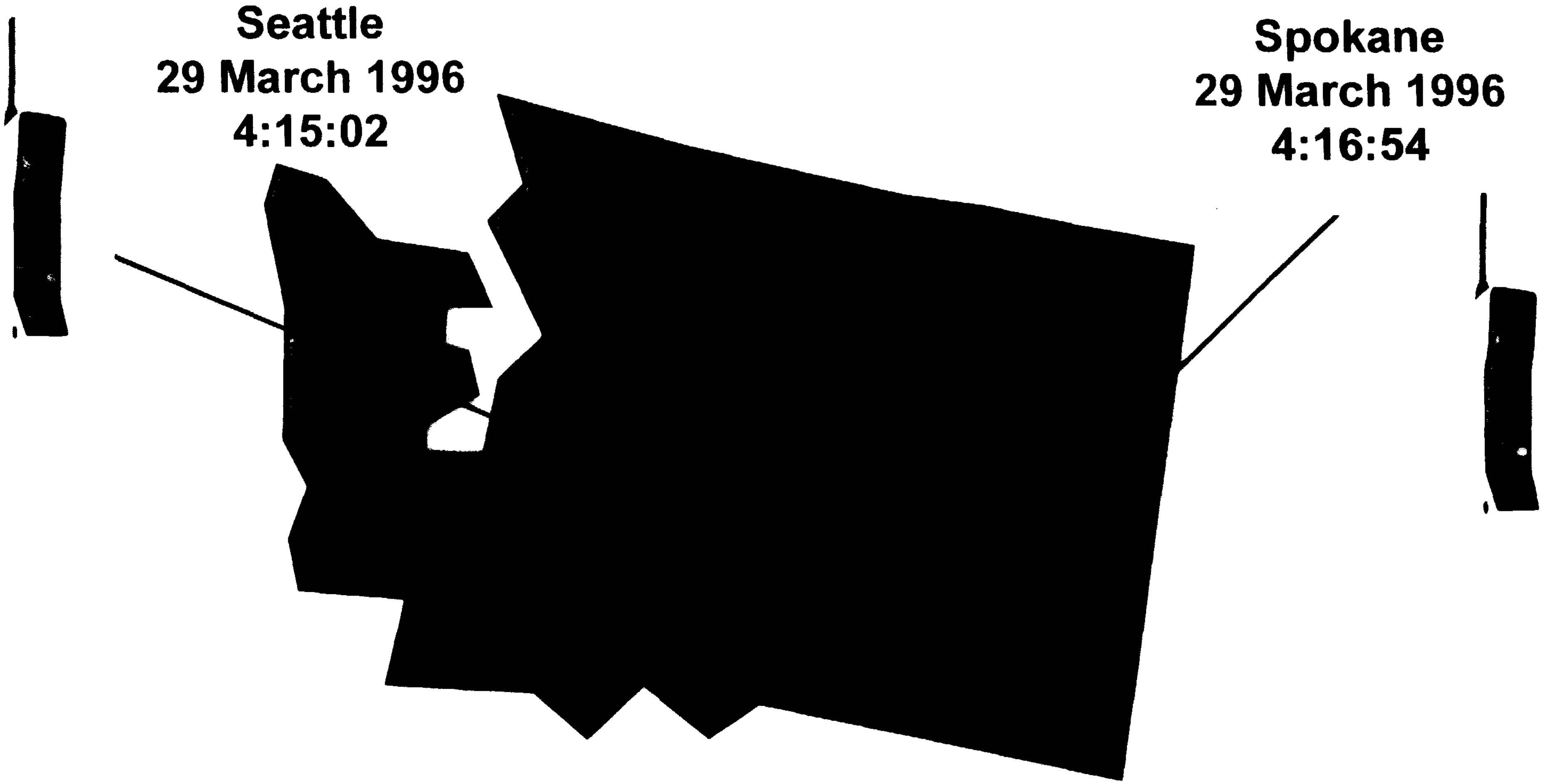
- Time-based validation systems
- Radio frequency (RF) signature technology
- Voice verification technology
- Dynamic password technology
- Cryptographic authentication techniques

Principle of Profiling System



AT&T Wireless Services

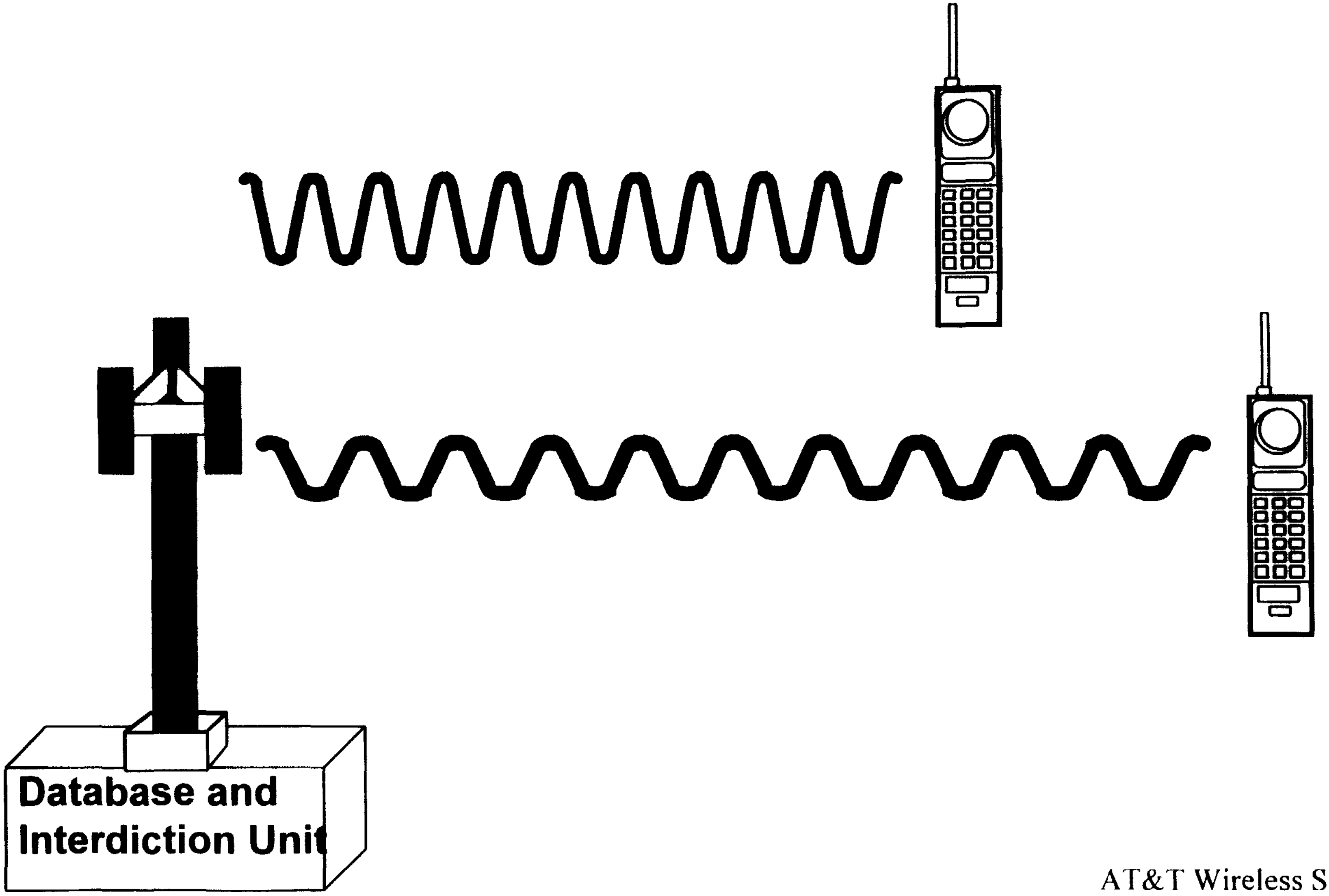
Velocity Checking – An Example



Seattle
29 March 1996
4:15:02

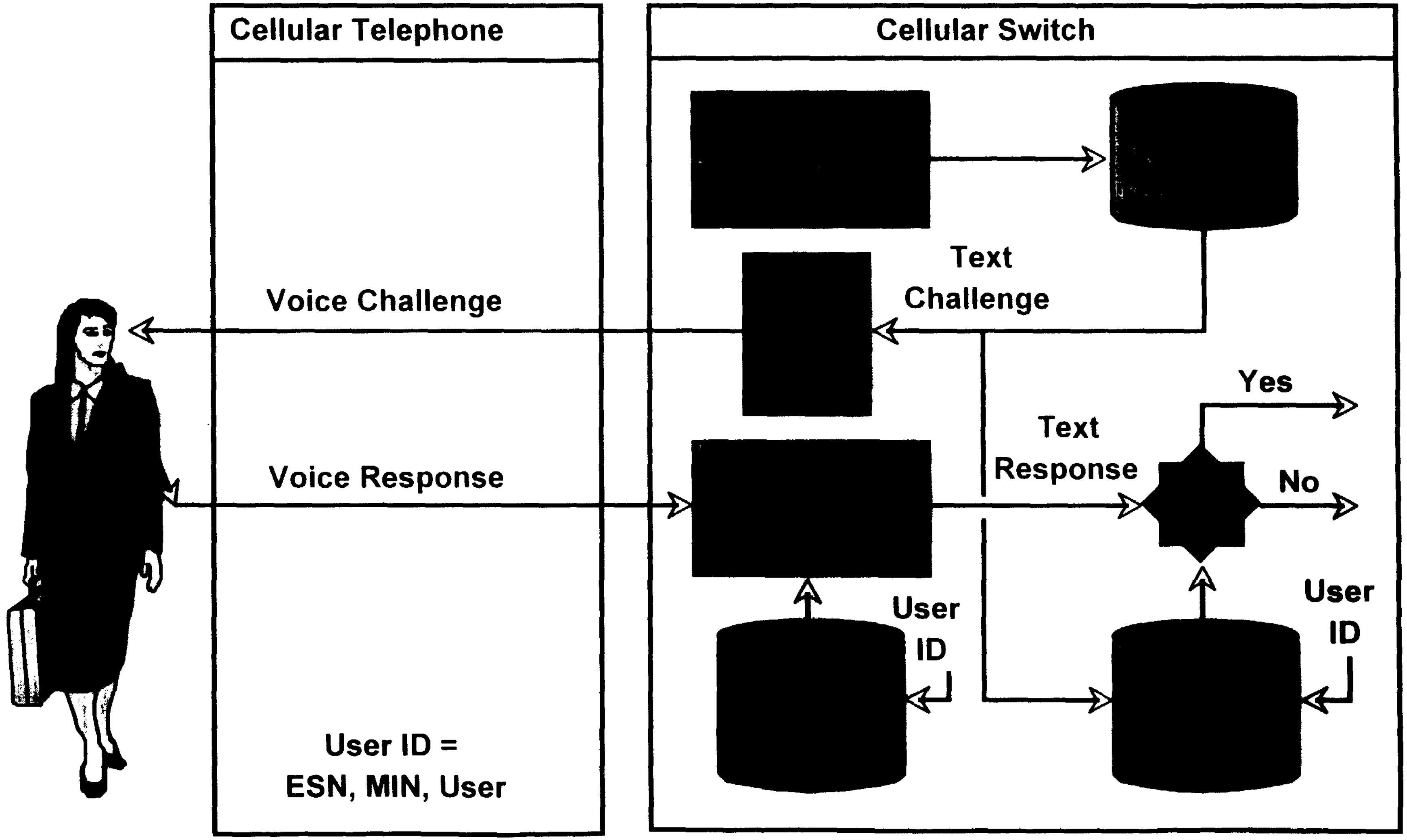
Spokane
29 March 1996
4:16:54

RF Fingerprinting Technology - Per cell site

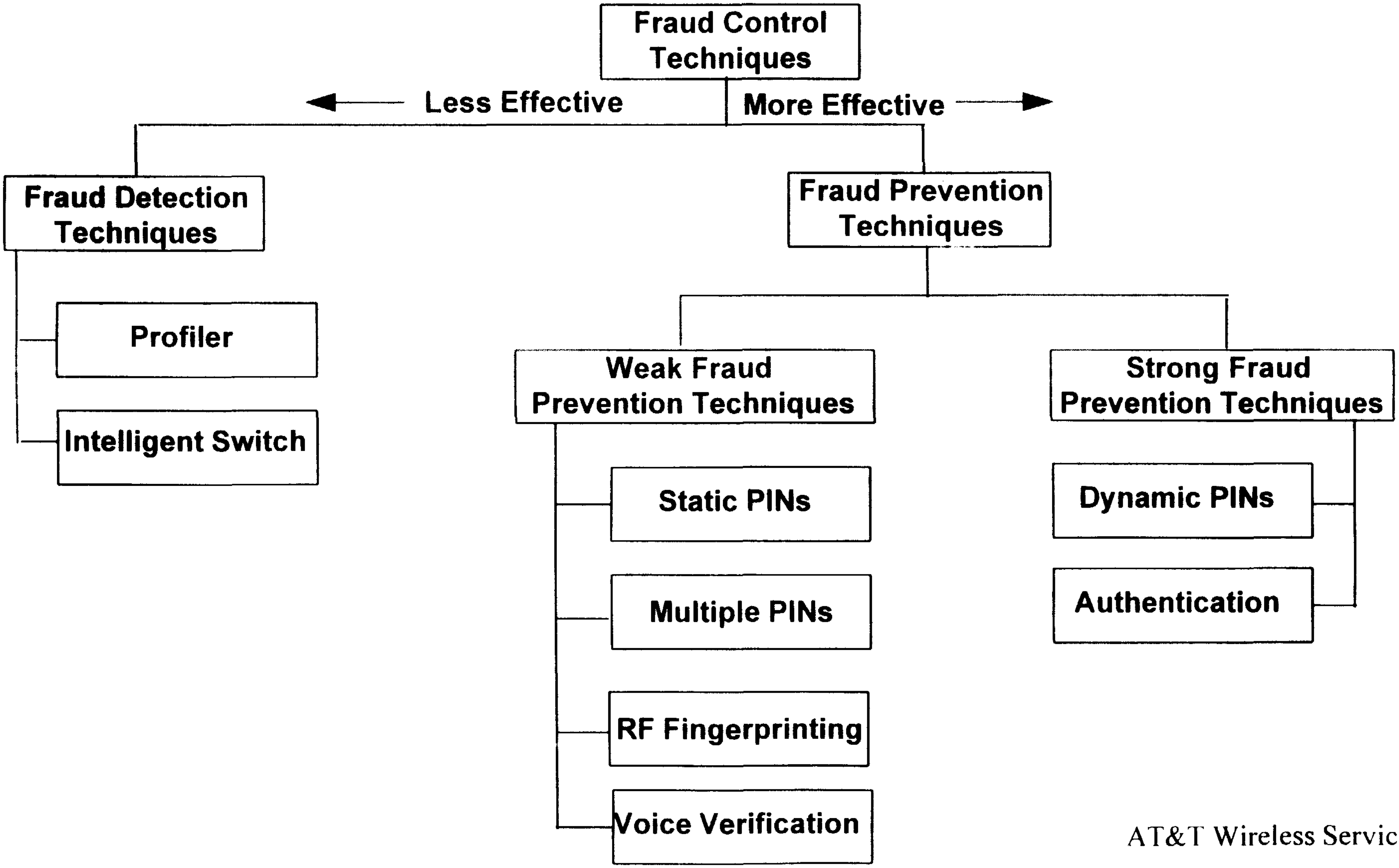


Database and Interdiction Unit

Principle of Cellular Authentication Using Voice Verification



Taxonomy of Fraud Control Techniques



Fraud Control Techniques

← Less Effective

More Effective →

Fraud Detection Techniques

- Profiler
- Intelligent Switch

Fraud Prevention Techniques

Weak Fraud Prevention Techniques

- Static PINs
- Multiple PINs
- RF Fingerprinting
- Voice Verification

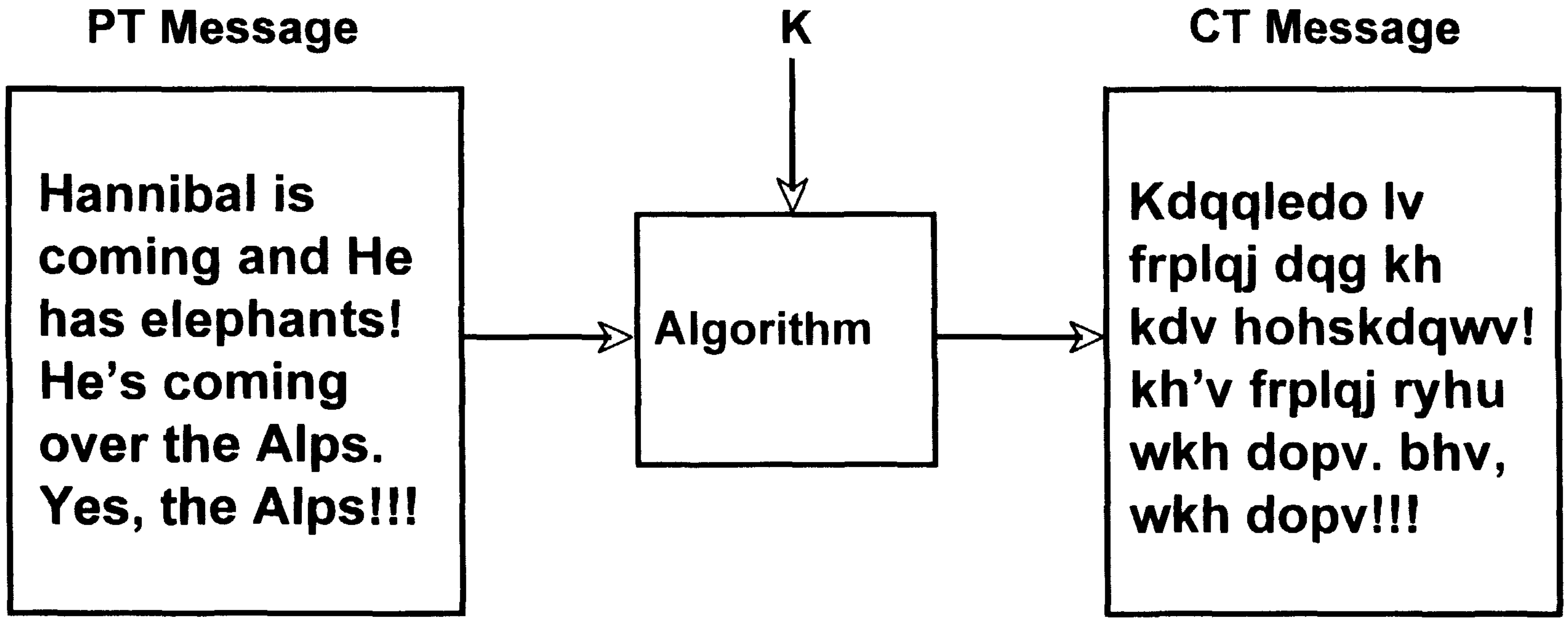
Strong Fraud Prevention Techniques

- Dynamic PINs
- Authentication

Cryptology — Basic Concepts

- **Cryptology**
  - Science that embraces both cryptography and cryptanalysis
- **Cryptography**
  - Art (or science) of secret writing
  - Includes means for performing all "security services"
- **Cryptanalysis**
  - Attempt to descramble or scramble without knowledge of secret key

Example of Simple Cryptographic System



PT Message

Hannibal is coming and He has elephants! He’s coming over the Alps. Yes, the Alps!!!

K

Algorithm

CT Message

Kdqqledo lv frplqj dqg kh kdv hohskdqwv! kh’v frplqj ryhu wkh dopv. bhv, wkh dopv!!!

700–90

History of Cryptography

- Circa. 1900 B.C. — Birth of Cryptology
  - Egyptians use hieroglyphic symbols to document history
- 50 B.C.
  - Julius Caesar writes to friend Cicero using the "Caesar alphabet"
- Middle Ages
  - Geoffrey Chaucer uses symbol cipher in several works
- Late 1700's
  - Thomas Jefferson — the Father of American Cryptography develops "cypher wheel"

History of Cryptography (cont'd)

- **Civil War Period**
  - **Armies use "word transposition" cryptography to protect military communications**
- **1926**
  - **Vernam develops concept of "one-time pad" telegraph cipher**
- **World War II Period**
  - **U.S. uses Hagelin (Converter M-209) for military communications**
- **1974**
  - **IBM develops Data Encryption Standard (DES)**
- **1995**
  - **U.S. introduces authentication for cellular**

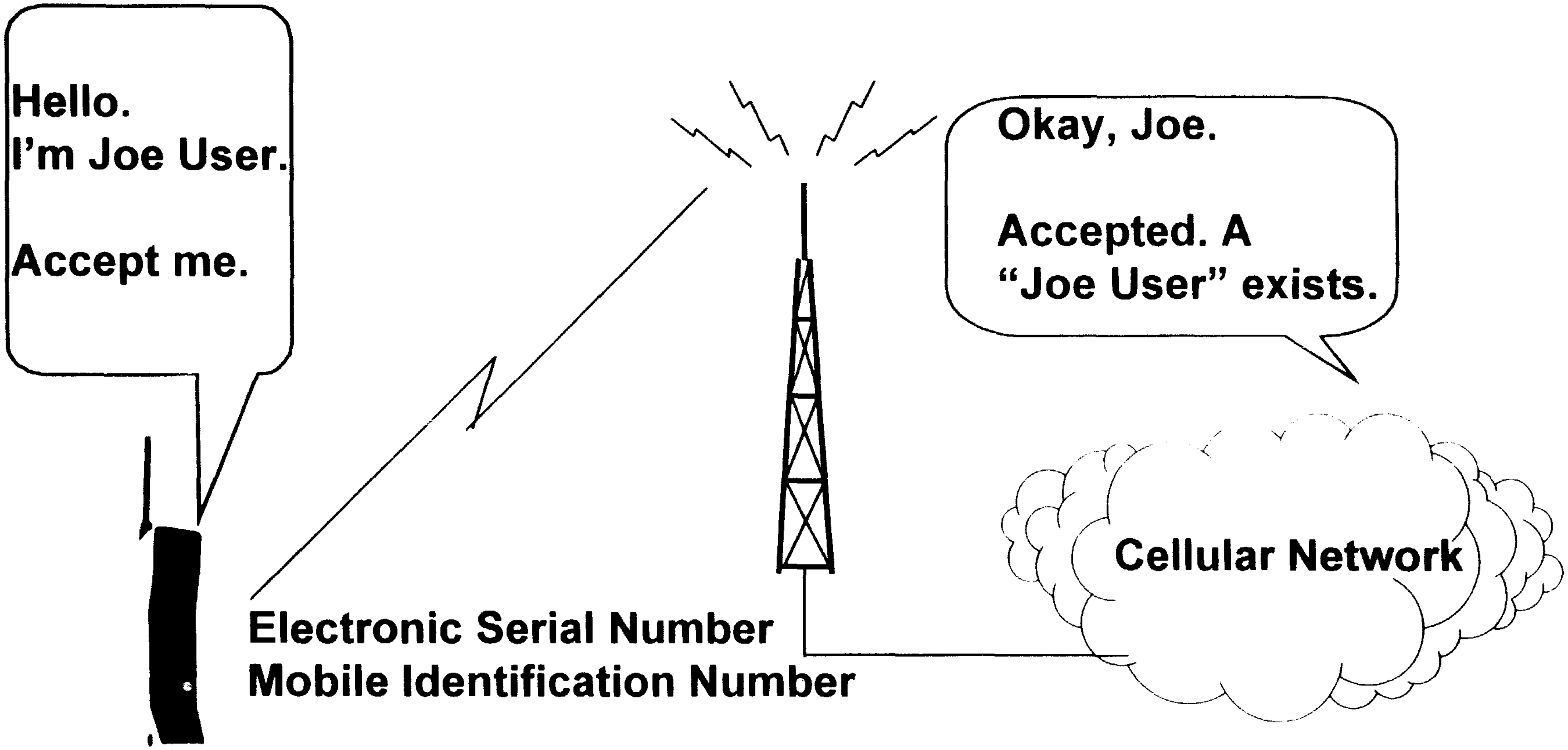
Authentication ... A Closer Look

Money Dispensing at ATM Machine — Everyday Authentication

Fundamental Definitions

- **Identification**
  - — **Process whereby the cellular network recognizes a subscriber's identity over the radiopath**
  - — **Analogous to a computer *UserID***
- **Authentication**
  - — **Process whereby the cellular network verifies the claimed identity of a subscriber to protect the network against unauthorized use (theft of service)**
  - — **Analogous to a password associated with the UserID**
  - — **In the cellular environment, the password is "dynamic": changing on every access attempt**

Current Cellular "Identification" Scheme



Hello.
I'm Joe User.

Accept me.

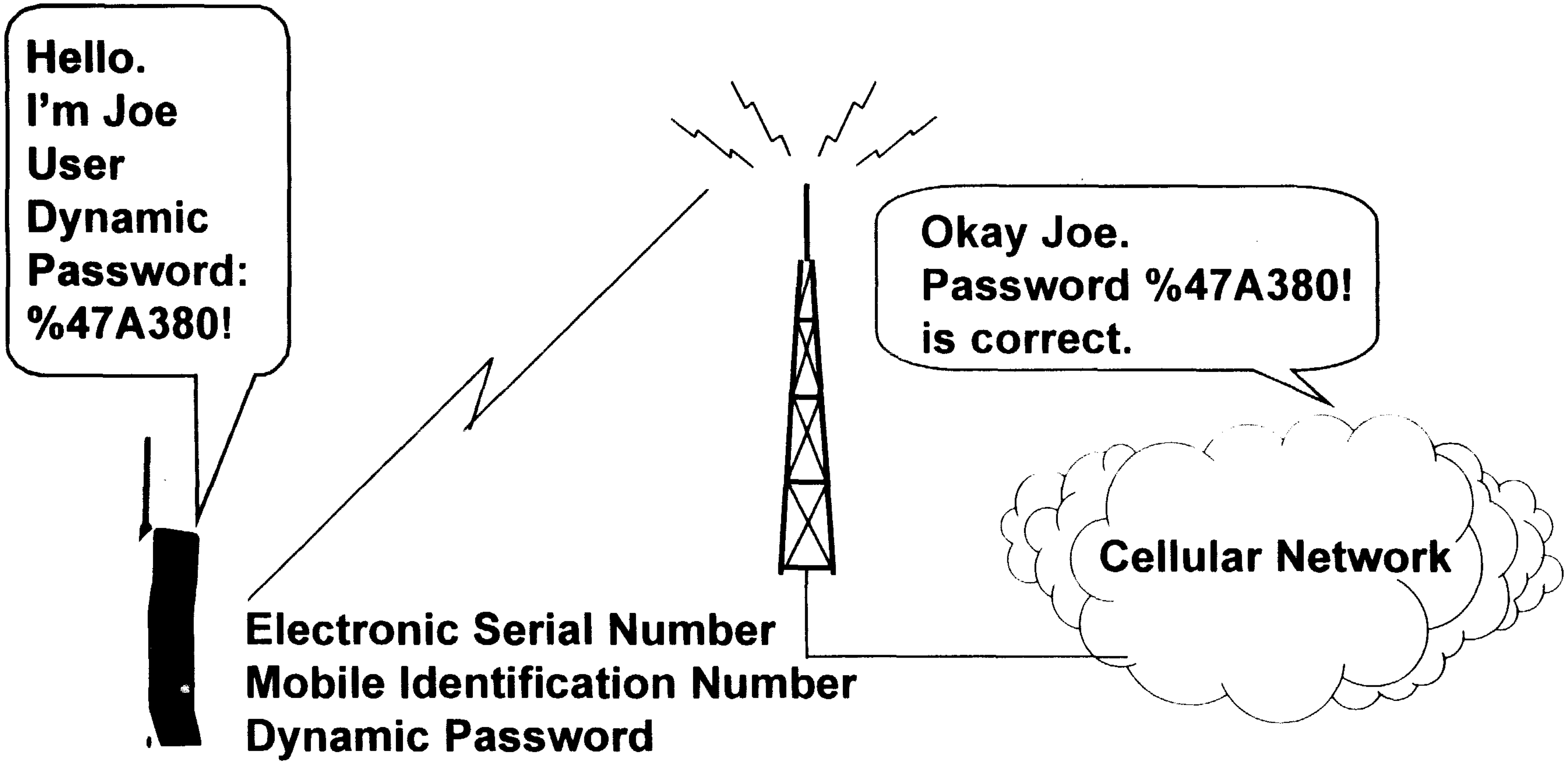
Okay, Joe.

Accepted. A "Joe User" exists.

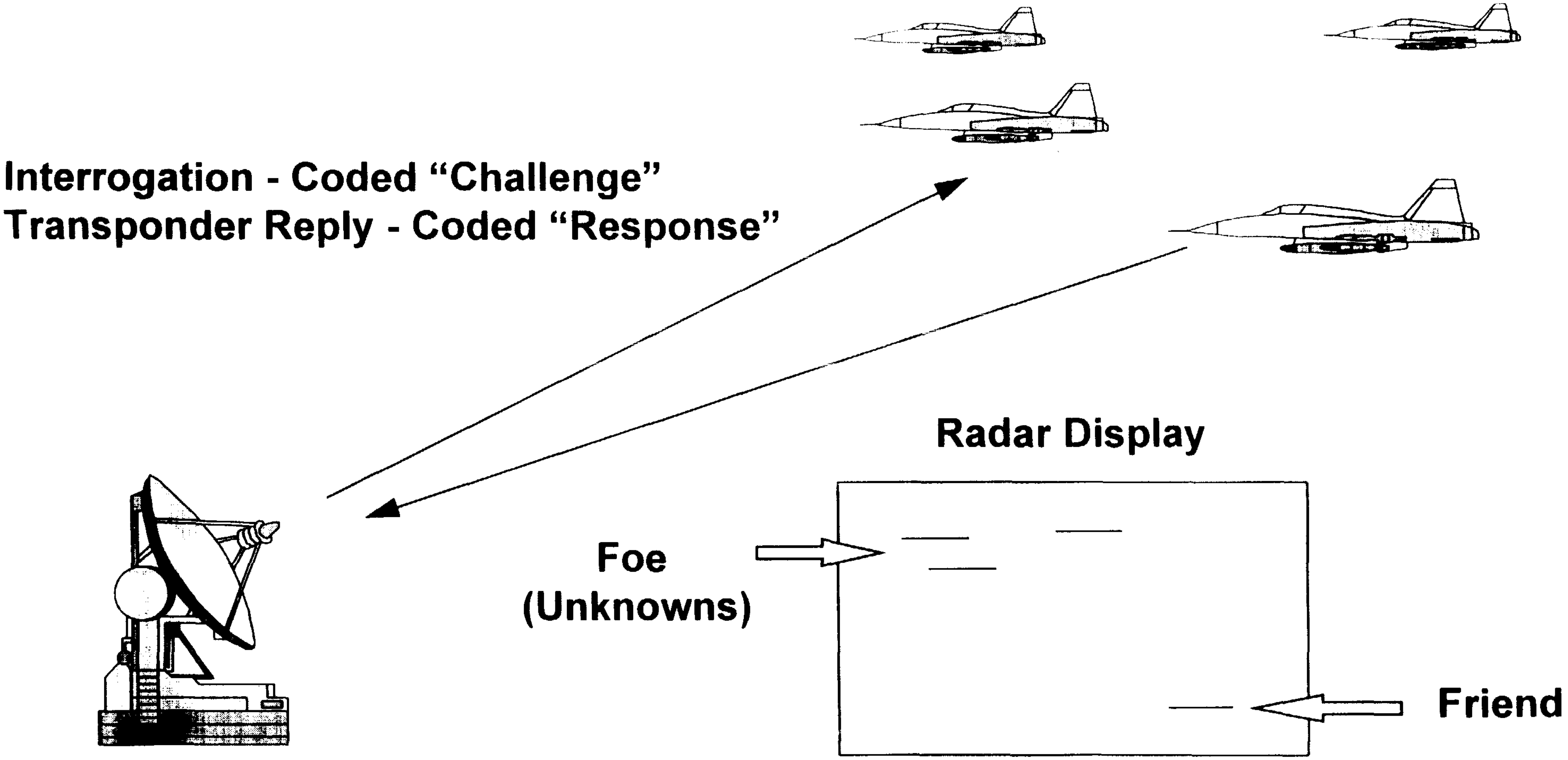
Cellular Network

Electronic Serial Number
Mobile Identification Number

Cellular Challenge-Response "Authentication" Scheme



Basic Principles of Identification, Friend, and Foe (IFF)



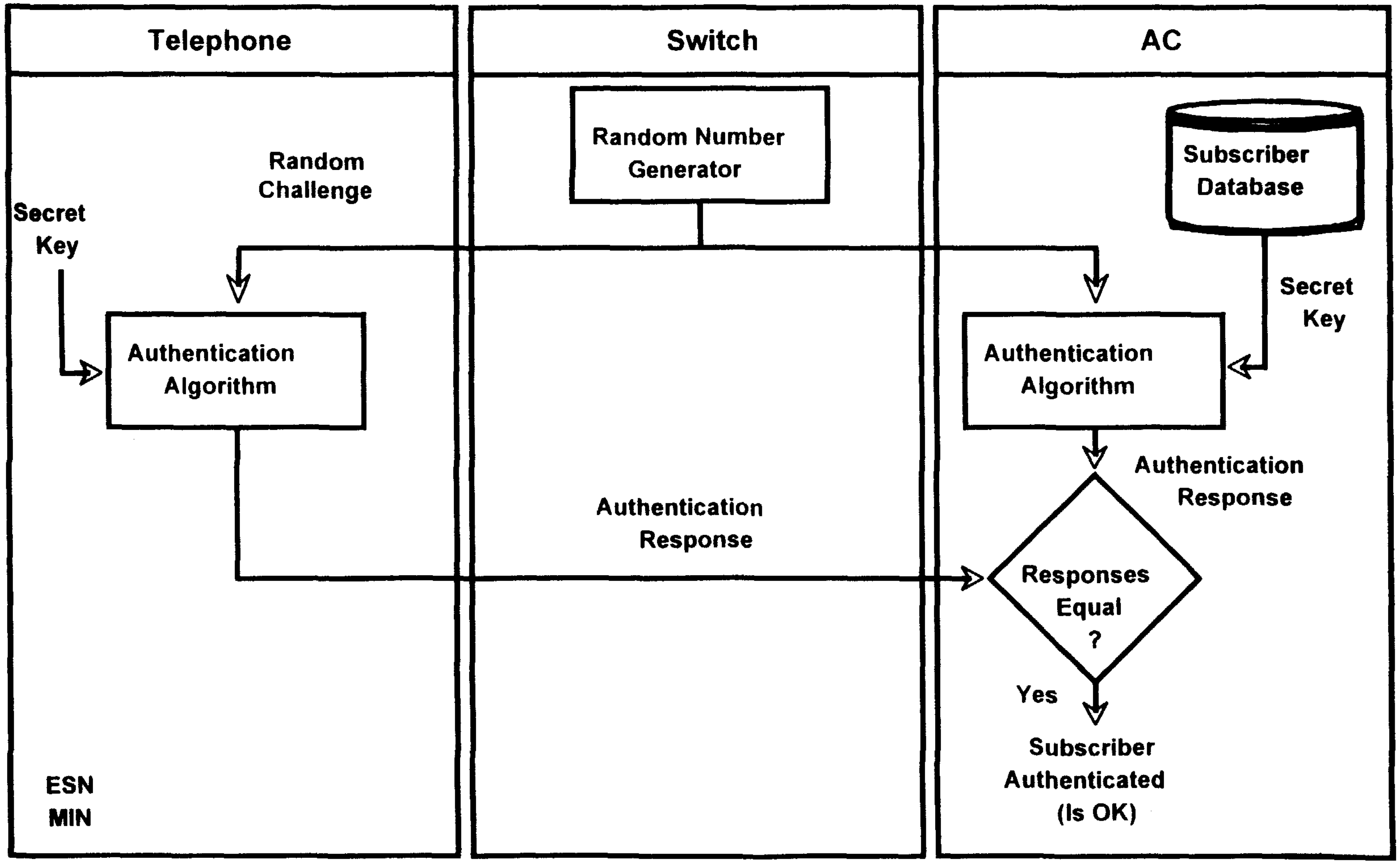
Interrogation - Coded "Challenge"
Transponder Reply - Coded "Response"

Radar Display

Foe
(Unknowns)

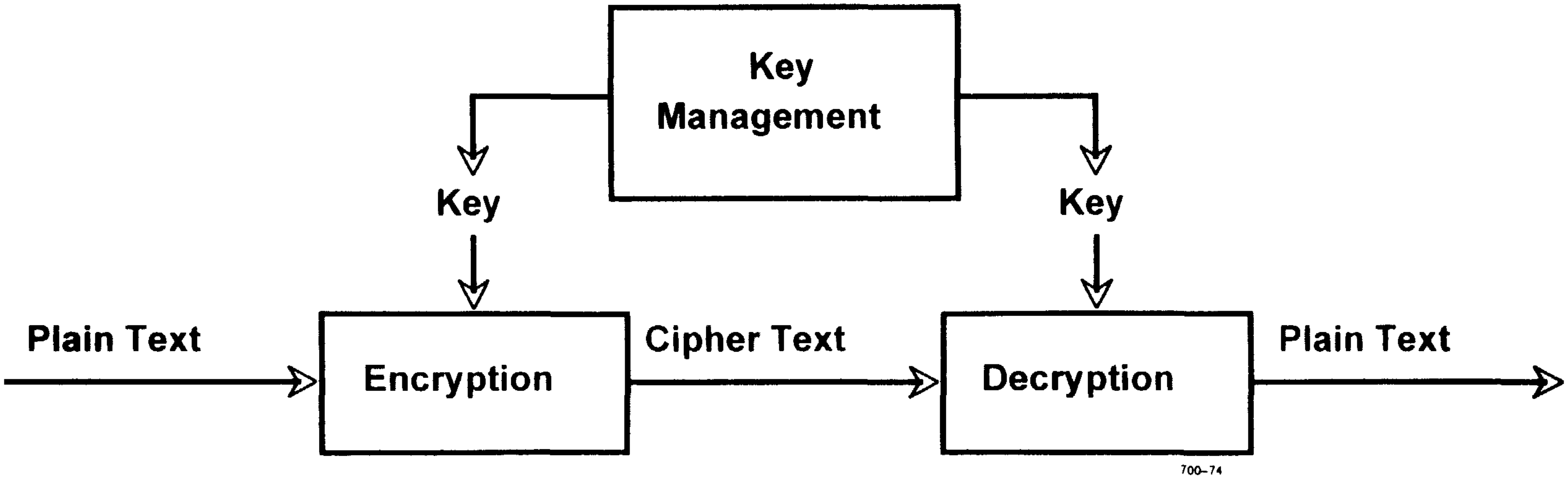
Friend

Principle of Cellular Authentication



700–63

Cryptographic Key Management



"The generation, distribution/issuance, storage, updating, destruction, and archiving of keys"